UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA, v. VLADISLAV KLYUSHIN, a/k/a "Vladislav Kliushin" Defendant.	21-CR-10104-PBS/MBB

MEMORANDUM OF THE UNITED STATES IN SUPPORT OF DETENTION

Cantonal authorities arrested defendant Vladislav Klyushin in March 2021, minutes after he arrived by private jet in Sion, Switzerland. A helicopter had been waiting on the tarmac to take him and his party to Zermatt, an exclusive ski resort nearby. The defendant, who is accused of making tens of millions of dollars on illegal stock trades using financial information stolen from U.S. computer networks, was detained in Switzerland, where he vigorously opposed his extradition. So did the Russian government, a customer of the defendant's Moscow-based company, M-13, which offers services that emulate computer network attacks.

Now extradited to the United States—a country with which he has no ties—the defendant faces charges and a Guidelines sentencing range that could imprison him for more than 20 years. The defendant's lack of ties to this District, the seriousness of his offense, his immense wealth, his ties to the Russian government, and that government's stated desire to return him home all combine to create a serious risk that the defendant will flee the United States, will not appear for trial, and will return to Russia—a country with which the United States has no extradition relationship. Under these circumstances, there is no combination of conditions that will

reasonably assure the defendant's appearance, and the Court should detain him pending trial. *See* 18 U.S.C. § 3142(e).

I. Background

The Indictment charges the defendant and two other Russian nationals, Ivan Ermakov and Nikolai Rumiantcev, for their roles in a conspiracy to obtain unauthorized access to computer networks, and to commit wire fraud and securities fraud. (Indictment, Docket No. 8). Between approximately January 2018 and September 2020, the defendants and coconspirators used stolen usernames and passwords to access the computer networks of Filing Agent 1 ("FA 1") and Filing Agent 2 ("FA 2"), and to view and download material non-public information ("MNPI") about the financial performance of publicly traded companies, before that information was filed with the Securities and Exchange Commission ("SEC") or announced to the general public. Armed with that information, the defendants and others enriched themselves by trading in the securities of those companies, generating tens of millions of dollars in profits. (Indictment, ¶ 12).

II. The Defendant Has No Ties to the District of Massachusetts

As the defendant testified at his initial appearance, all of his ties are outside the United States, most of them in Russia. His home, spouse, five children, employment, and educational and community ties—all factors the Court must consider under 18 U.S.C. § 3142(g)(3)(A)—are in Russia. There is no network of friends or family who could serve here as third-party custodians; no employment that he could be ordered to seek or maintain; and no permanent residence to which he could be ordered confined. Any ties to this District would be ones that the

defendant was able to purchase and control. Given his wealth described below, the defendant could just as easily leave these purchased ties behind.

III. The Defendant has the Means to Flee

The Indictment charges the defendant and his coconspirators with making tens of millions of dollars in illegal profits.[1] (¶ 12). The investigation to date has accounted for only a fraction of this amount, suggesting that the defendant and his coconspirators have stored the profits around the world and in countries beyond the reach of the United States. Financial records, described in FBI Special Agent B.J. Kang's affidavit in support of a criminal complaint, (Docket No. 1, hereinafter "Compl. Aff. ¶ __), reveal trading profits for the defendant and M-13 in Russia, the United Kingdom, Denmark, and Cyprus, with a coconspirator also trading through an account at a Portuguese financial institution. (Compl. Aff. ¶¶ 8c, 8d, 8e, 69, 94, 95).

Below are photographs that the defendant shared with his co-defendant and employee, Ermakov, in August 2019. The pictures, taken at different times, show a single safe containing an increasing amount of U.S. one hundred dollar bills. Based on the amount of currency in the safe on the right, and a comment that the defendant made to Ermakov that the amount in the safe is about "3," investigators believe that safe—whose exact location is unknown—may have contained as much as $3 million in cash. (Indictment, ¶ 31).

[1] A Securities and Exchange Commission complaint charging each of the five coconspirators pegs the total illegal profits from the scheme at approximately $82.5 million. *SEC v. Klyushin et al.*, 21-cv-12088 (D. Mass. filed Dec. 20, 2021), Docket No. 1 at 2.


Electronic communications and other records seized during the investigation similarly reveal that in March 2020, Klyushin paid more than three million British pounds (~$3.97 million) for a 77 ½ foot luxury motor yacht, "Seven K", using the same Russian Standard Bank account that funded trading in furtherance of the conspiracy.

INVOICE

Klyushin Vladislav Dmitrievich
Arbat street, 13/36, bld 2, ap. 5
MOSCOW
RUSSIAN FEDERATION

Invoice Date
5 Mar 2020

Invoice Number
INV-0133

Reference
BN 1652076

Yacht Trading Group CIS Limited
Elenion Building, 5
Themistokli Dervi
NICOSIA CYPRUS
CY-1066
CYPRUS
TIC: 10381095P
CY VAT: 10381095P
MT VAT: MT26195319
FR VAT: FR02878095439

Description	Quantity	Unit Price	Tax	Amount GBP
Total Price of Sunseeker 76 Yacht BN 1652076 per Assignment Agreement to SPA SS/76Y/1652076 dd 04 February 2020	1.00	3,056,295.00	Tax Exempt	3,056,295.00

The defendant's assets, some unaccounted for and many beyond the reach of U.S. authorities, provide him with a financial reservoir that could fund his flight if released. Private planes, helicopters, yachts, and piles of cash are the working tools of someone with sufficient

incentive to flee. For the reasons stated below, the United States submits that the defendant has that incentive.

IV. The Weight of the Evidence Against the Defendant is Substantial

Financial and electronic records obtained during the course of the investigation make clear that the defendant and his coconspirators accessed MNPI stored on the networks of FA 1 and FA 2, and that they profited by trading on that information in advance of announcements of publicly traded companies' performance.

The complaint affidavit attributes the unauthorized access to the victims' networks to M-13, and to Ermakov specifically. (Compl. Aff. ¶¶ 16-17). Ermakov, a former Russian military intelligence officer, worked for the defendant at M-13 as a deputy general director. (Compl. Aff. ¶¶ 8b & n.3). Ermakov's hacking credentials are extensive. He is separately accused in two other United States indictments with hacking, influence, and disinformation efforts targeting the 2016 U.S. elections, international anti-doping agencies, sporting federations, and anti-doping officials. (Compl. Aff. ¶ 8a & n.3). In this matter, the evidence will show that, on or about May 9, 2018, starting at approximately 3:46 a.m. (ET), Ermakov used a stolen username and password to access FA 2's computer from an IP address that, within two minutes, was also used to update applications on one of Ermakov's internet-connected devices. (Compl. Aff. ¶¶ 16-17).[2] Over that IP address, Ermakov viewed or downloaded earnings-related files of four companies—Cytomx Therapeutics, Horizon Therapeutics, Puma Biotechnology and Synaptics—

[2] The investigation linked internet infrastructure used in the compromise of FA 1's network to IP addresses that the defendant, Ermakov, and Rumiantcev each used on several occasions between November 2018 and September 2020.

each of which reported quarterly earnings later that day. (Compl. Aff. ¶¶ 17). That same stolen username and password combination was used hundreds of times between February 2018 and January 2020 to gain unauthorized access to FA 2's computer network and to view or download MNPI of companies in whose securities the defendant and his coconspirators traded. (*E.g.*, Compl. Aff. ¶¶ 48, 82, 85, 90).

Electronic records obtained during the investigation indicate that, on or about January 23, 2020—two days after an FA 1 employee's compromised login credentials were used to view or download drafts of Avnet's earnings disclosure on FA 1's computer network—Ermakov used SaxoTraderGO, a mobile trading app for Saxo Bank clients, to access Klyushin's account at Saxo, a Danish investment platform, to short Avnet using "contracts for difference" ("CFDs"), which are a type of security that allows traders to participate in the price movement of a stock without actually owning the stock itself. (Compl. Aff. ¶ 68). Brokerage records indicate that Mikhail Irzak, a coconspirator, shorted Avnet that same day in one of his brokerage accounts. After the stock market closed, Avnet reported second quarter financial results that fell short of market expectations. (Compl. ¶¶ 60-61).

As another example, computer forensic data indicates that, on or about November 1, 2019, and again between November 4 and November 6, 2019, intruders gained unauthorized access to Roku, Inc.'s earnings-related files on FA 2's computer network. (Compl. Aff. ¶¶ 13, 86). Brokerage records indicate that, on November 6, 2019, between 11:57 a.m. and 3:59 p.m. (ET), the defendant sold short 42,500 Roku CFDs in his Saxo account. (Indictment, ¶ 32). That same day, Irzak sold short 5,000 Roku shares in his Interactive Brokers account. After the stock market closed later that day, Roku reported third quarter financial results and reduced its profit forecasts,

resulting in a steep decline in its stock price. The defendant thereafter covered his short position for a profit of approximately $1 million, and his co-conspirator Irzak did the same, earning approximately $87,000. (Indictment, ¶ 34).

As a third example, on or about July 28, 2019 and July 29, 2019, intruders gained unauthorized access to the earnings-related files of SS&C Technologies, Inc. ("SSNC") on FA 2's computer network. (Compl. Aff. ¶ 85). Brokerage records indicate that on or about July 29, 2019, between approximately 3:08 p.m., and 3:52 p.m. (ET), the defendant sold short in his Saxo account 11,800 SSNC CFDs. (Indictment, ¶ 28(d)). (After the stock market closed, SSNC reported second quarter financial results and lowered its profit forecasts. The next day, July 30, 2019, the defendant covered his entire SSNC short position for a profit of approximately $114,000. (Indictment, ¶ 29). Brokerage records indicate that Irzak likewise shorted SSNC shares in two brokerage accounts and then covered his short positions for a combined profit of approximately $212,000. (Indictment,¶ 28)

Communications seized during the investigation make clear that the defendant was involved in the trading and aware of the source of the information. For example, on February 21, 2020, just after the Avnet trading described above, the defendant and Ermakov exchanged messages in which the defendant asked, "Let me help you with saxo," and Ermakov replied "I [can do it] myself". (Compl. Aff. ¶ 68 & n.14).

Similarly, on or about October 24, 2018—just hours after intruders gained unauthorized access to Tesla's draft earnings release on FA 2's network, and the same day that both the defendant and Irzak purchased shares of Tesla in their respective brokerage accounts, the defendant sent the following message to two individuals whose investment accounts M-13

controlled (and whose accounts had traded in parallel with the defendant and Irzak): "Pay attention to shares of Tesla now and tomorrow after 16:30 and on how much they go up." The defendant sent this message when Tesla's financial results were still non-public. Tesla later reported positive third quarter financial results after the market closed that day. (Compl. Aff. ¶¶ 72-73.).

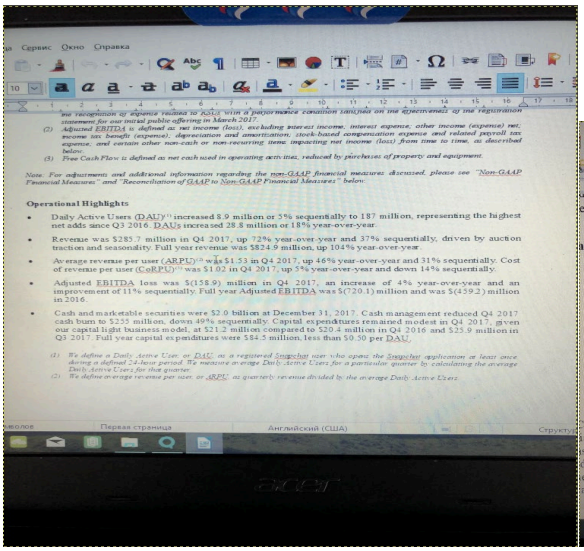
The defendant and Ermakov later congratulated each other on profits they had earned for the M-13 investors. In a text message exchange approximately seven months after the Tesla trading, the defendant reported to Ermakov that one investor had made profits of close to $1 million over that period, nearly tripling his investment, and that a second had made profits of close to $700,000, nearly doubling his investment. The defendant added: "They don't even ask why so anymore [smile]." (Compl. Aff. ¶ 77).

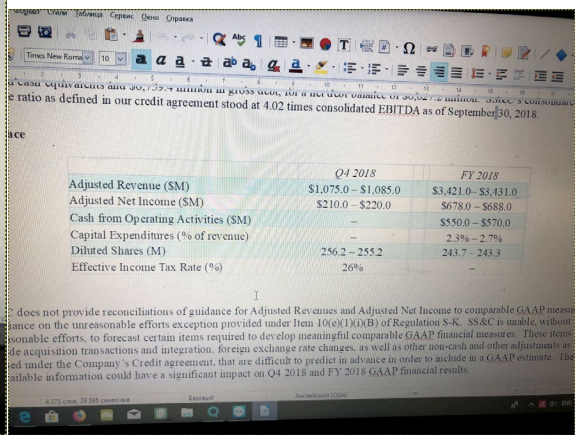
In another text message exchange recovered during the investigation, the defendant and Ermakov discussed buying real estate with the proceeds of their trading. The defendant and Ermakov then had the following exchange (as translated in draft from the Russian).

KLYUSHIN:	if there's money it could be bought
KLYUSHIN:	i'm not ready
ERMAKOV:	Me too for now
KLYUSHIN:	key word for now [three smiles]
KLYUSHIN:	apartment is cool
ERMAKOV:	[winking face emoji]
KLYUSHIN:	*we'll earn and then we can buy [it]*
ERMAKOV:	*Need to go to work then [smile]*
KLYUSHIN:	*no need to*
KLYUSHIN:	*just turn on the computer*
KLYUSHIN:	*[three smiles]*
KLYUSHIN:	and give it a little thought [three smiles]
ERMAKOV:	I already thought yesterday
ERMAKOV:	Today I will think some more [smile]
KLYUSHIN:	[four loudly crying face emojis]

(Compl. Aff. ¶ 67 & n.13). Klyushin's reference to earning without needing to go to work demonstrates his knowledge of the source of the conspiracy's profits.

Photographic evidence obtained from an Internet Service Provider account of coconspirator Igor Sladkov's provides conclusive proof that the defendant and his coconspirators were in possession of stolen MNPI at the time they traded. For example, the two photographs below show portions of the draft earnings releases of two companies, Snap Inc. and SSNC, displayed on the screen of Sladkov's computer:





	Q4 2018	FY 2018
Adjusted Revenue ($M)	$1,075.0 – $1,085.0	$3,421.0 – $3,431.0
Adjusted Net Income ($M)	$210.0 – $220.0	$678.0 – $688.0
Cash from Operating Activities ($M)	–	$550.0 – $570.0
Capital Expenditures (% of revenue)	–	2.3% – 2.7%
Diluted Shares (M)	256.2 – 255.2	243.7 – 243.3
Effective Income Tax Rate (%)	26%	–

In total, there is substantial evidence linking the defendant and his coconspirators to the unauthorized access and to timely and profitable trading that followed. Under 18 U.S.C. § 3142(g)(2), the weight of the defendant's own words, trades, and profits suggest that he will be convicted at trial, and that he accordingly has substantial incentive to flee the United States.

V. The Defendant Faces a Substantial Term of Imprisonment Upon Conviction

As noted above, financial records indicate that the defendant and his four coconspirators earned in excess of $80 million trading in the securities of FA 1 and FA 2's public company clients. These losses to other investors, and the complex international nature of the defendant's alleged offense, provide for a Guidelines Sentencing Range of more than 20 years in custody. The defendant accordingly has little incentive to remain in this District to face these charges, but he has significant incentive to flee to Russia, a jurisdiction from which he cannot be returned.

Guideline	Base Offense Level	Adjustments
§ 2B1.1(a)(1)	7	
§ 2B1.1(b)(2)(M)		+24 (more than $65 million in loss)
§ 2B1.1(b)(10)(B)		+2 (substantial part of offense committed outside U.S.)
§ 2B.1.(b)(18)		+2 (conviction under 18 U.S.C. § 1030 involving personal information)
§ 3B1.1(a)		+4 (organizer/leader, 5+ participants, otherwise extensive offense)
Total Offense Level	39	262 to 327 months

VI. The Defendant's Extradition to the United States Counsels Detention

The defendant did not come here voluntarily. He was arrested in Switzerland, where he fought the United States' extradition request for more than eight months. According to press reports, that included at least two appeals from the decision of the Swiss Ministry of Justice ordering his extradition, the last of which went to the Swiss Federal Tribunal, that country's highest court. Notably, Swiss authorities felt it necessary to seek and secure the defendant's detention during his extradition proceedings. While the defendant was clearly entitled to oppose extradition, the Court should not ignore the fact that he is in Massachusetts against his will.

The Russian government—from whom the defendant received the Medal of Honor pictured below (with translation annotated)[3] and bearing the signature of the President of the Russian Federation—also wants the defendant out of Massachusetts. According to press reports, it filed a competing request for the defendant's extradition to Switzerland shortly after he was arrested—a tactic Russia has used in other extradition matters involving its citizens arrested abroad. *A New Russian Ploy: Competing Extradition Requests*, N.Y. TIMES (Dec. 20, 2017) (https://www.nytimes.com/2017/12/20/world/europe/russia-extradition-levashov.html) (visited Dec. 21, 2021).

What results is a combination of wealth—both the defendant's and his government's—and a demonstrated intent to avoid his having to face charges here. For a defendant with no ties in Massachusetts and every reason to want to be elsewhere, there are no conditions short of detention that cannot be circumvented. There is little to suggest that a significant bond or a location monitoring device would adequately assure the defendant's appearance. If the defendant flees to Russia, whether by air or sea, there will be no mechanism for the United States

3

to seek his return. *See United States v. Dermen*, 779 Fed. Appx 497 (10th Cir. 2019) (reporting district court's flight risk finding based on, among other things, the defendant's ownership of a yacht, overseas bank accounts, overseas residence, access to a private plane; and the Turkish President's public commitment not to honor extradition requests from the United States). There is accordingly no combination of conditions that would reasonably assure the defendant's appearance. The Court should order him detained pending trial.

Respectfully submitted,

NATHANIEL R. MENDELL
Acting United States Attorney

By: */s/Seth B. Kosto*
STEPHEN E. FRANK
SETH B. KOSTO
Assistant U.S. Attorneys

Date: December 21, 2021